

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

-----X
UNITED STATES OF AMERICA :

-v.- : **07 Cr. 913 (KMK)**

PHILIP ETKIN, :

Defendant. :
-----X

**GOVERNMENT’S MEMORANDUM OF LAW IN OPPOSITION TO
DEFENDANT’S MOTION TO PRECLUDE THE GOVERNMENT FROM
INTRODUCING INTO EVIDENCE AN EMAIL SENT BY THE DEFENDANT TO HIS
WIFE AND FOR A TAIN T HEARING**

PRELIMINARY STATEMENT

The Government respectfully submits this memorandum of law in opposition to defendant’s motion to: (1) preclude the Government from introducing into evidence an email, sent from the defendant’s official work email and found in the defendant’s official government car; and (2) dismiss the indictment or hold a “taint” hearing because the Government has viewed the email. Defendant’s motion should be rejected. First, it is clear that the email that the defendant sent to his wife was not a “confidential communication” and therefore is not protected by the marital privilege. Further, assuming arguendo that the email is protected by the marital privilege, there is no basis for either the Indictment – which was returned by the grand jury prior to the discovery of the email – to be dismissed or for a “taint” hearing to be held. Accordingly, defendant’s motion should be denied without hearing.

RELEVANT FACTS

The defendant is charged in a one count Indictment with violating the Hobbs Act. Specifically, the defendant is charged with attempting to extort \$3,500 from an individual in Middletown, New York, in exchange for preventing a purported act of violence against the individual. The Indictment was returned on September 27, 2007 and a warrant was issued that day for the defendant's arrest.

On the morning of September 28, 2007, the defendant, while driving a car provided to him by the New York State Police ("NYSP") for official government business, was arrested by FBI agents. During an inventory of the car, FBI agents recovered numerous documents including a print out of a March 13, 2007 email sent from the defendant – using his official email address – to his wife. (Attachment to Def.'s Aff.).¹

ARGUMENT

I.

DEFENDANT'S EMAIL IS NOT WITHIN THE SCOPE OF THE MARITAL COMMUNICATIONS PRIVILEGE

Contrary to the defendant's argument, his March 13, 2007 email discussing his commission of a crime is not protected by the marital communications privilege for three reasons: (1) the Etkins were separated at the time of the email; (2) the email was not a

¹ The Government has no intention of offering the email from Etkin's wife to Etkin and would seek to offer, pursuant to Fed. R. Evid. 404(b), the portion of Etkin's email to his wife – on the second page of the Attachment to the Defendant's Affidavit – that begins with "Also on another note" and ends with "but im sure it will" and would redact the name of the individual mentioned in that portion of the email. See Fed. R. Evid. 404(b) (Evidence is admissible to prove, among other things, the defendant's "motive . . . intent, preparation, plan, knowledge . . . or absence of mistake or accident.").

confidential communication; and (3) assuming that the email was a privileged communication at the time of its creation, the privilege has since been waived.

The Federal Rules of Evidence do not explicitly provide for a marital privilege. Rule 501, however, provides that privileges are to be governed by common law principles, interpreted in light of reason and experience. In accordance with Rule 501, courts have recognized two marital privileges: “the testimonial privilege which permits one spouse to decline to testify against the other during the marriage, and the marital communications privilege which either spouse may assert to prevent the other from testifying to confidential communications made during the marriage.” United States v. Bahe, 128 F.3d 1440, 1442 (10th Cir. 1997).

The marital communications privilege provides that “[c]ommunications between the spouses, privately made, are generally assumed to have been intended to be confidential, and hence are privileged.” Wolfe v. United States, 291 U.S. 7, 14 (1934). Courts have generally held that the privilege: (1) extends to words and acts intended to be a communication; (2) requires a valid marriage; and (3) applies only to confidential communications. United States v. Vo, 413 F.3d 1010, 1016 (9th Cir. 2005). Because the privilege impedes the search for truth, the privilege is to be narrowly construed. See Trammel v. United States, 445 U.S. 40, 50 (1980); Vo, 413 F.3d at 1016 (“We construe the marital communications privilege narrowly, to promote marriage without thwarting the administration of justice.”).

A. The Email Was Sent While the Defendant And His Wife Were Permanently Separated And Is Not Protected By The Marital Privilege.

In United States v. Cameron, 556 F.2d 752 (5th Cir. 1977), the Court of Appeals for the Fifth Circuit held that the defendant's wife could not invoke the marital testimonial privilege

where the spouses were living apart and the marriage “was moribund.” In doing so, the Court noted that, because the marriage “as a social fact . . . had expired,” application of the privilege would in no sense “preserve domestic harmony.” *Id.* at 756. Similarly, in United States v. Byrd, 750 F.2d 585, 593 (7th Cir. 1984), the Seventh Circuit upheld the admission of testimony by the defendant's wife concerning statements made by the defendant to his wife during their permanent separation. The court held “that only communications that take place during a valid marriage between couples still cohabiting pursuant to that marriage are protected by the privilege.” *Id.* (emphasis added). The court reasoned that “[t]he importance of the search for truth at issue in a criminal trial outweighs the interest in protecting separated couples’ confidentiality.” *Id.*

Since Byrd, courts have consistently refused to apply the privilege to spousal communications made during a permanent separation. *See, e.g., United States v. Singleton*, 260 F.3d 1295, 1301 (11th Cir. 2001) (concluding that a district court in determining whether spouses are permanently separated at the time of the communication should consider “(1) Was the couple cohabiting?; (2) if they were not cohabiting, how long had they been apart; [] (3) had either spouse filed for divorce? . . . [and (4)] other objective evidence of the parties’ intent or lack of intent to reconcile.”); United States v. Murphy, 65 F.3d 758, 761 (9th Cir. 1995) (“factors include the duration of the separation, the stability of the marriage at the time of the communication, whether a divorce action had been filed and the conduct of the parties since that filing, whether a property settlement had been proposed, and, finally, any statements by the parties regarding irreconcilability or the reasons for separation”); United States v. Porter, 986 F.2d 1014, 1019 (6th Cir. 1993) (holding that “a district court should, when faced with this issue, make a factual determination as to whether the spouses were permanently separated at the time of the questioned

communication,” cautioning that a district court need not “consider any particular factors” and concluding that the marital communication at issue there was admissible because the wife had moved out ten to twelve days prior to the communication, there was no contact between the couple during the wife's hospital stay immediately prior to the separation, and, in hindsight, the separation was permanent); United States v. Treff, 924 F.2d 975, 982 (10th Cir. 1991) (upholding introduction of statements made by defendant to his wife and recorded in her diary on the basis that the couple had been separated for four months, both spouses filed for divorce shortly after the communication, and, during the separation, the husband dated other women and became engaged); United States v. Roberson, 859 F.2d 1376, 1381 (9th Cir. 1988) (holding that district courts should undertake a “detailed investigation into the irreconcilability of the marriage” if the couple is separated and “consider all . . . relevant circumstances” including the duration of the separation and the stability of the marriage at the time of the communication, whether a divorce action had been filed, the relationship of the spouses subsequent to the filing and prior to the communication, the spouses’ own statements about whether the marriage was reconcilable, and allegations of gross misconduct).

In In re Witness Before Grand Jury, 791 F.2d 234, 238 (2d Cir. 1986), the Second Circuit held that “a court may rely primarily on the duration of the couple’s physical estrangement, which is the guiding factor in determining ‘permanent separation.’” The Second Circuit stated: “The longer the period of estrangement at the time of the subject ‘communications,’ the easier it will be for the government to show that the couple, though still legally wed, had been in fact permanently separated and thus could not invoke the privilege.” Id. However, the court noted that “either party may bring forward special circumstances that render more or less likely the

objective possibility of reconciliation at the time of the communications.” Id.

Here, the Etkins were permanently separated at the time of the email. As set forth in Agent Presutti’s affidavit, it was the understanding of at least one of Etkin’s colleagues that the couple had been separated since approximately September 2006 – approximately six months before the email. (Exhibit A at ¶ 2). Further, on March 19, 2007, Etkin advised the NYSP that his official car would be parked at another residence, i.e. not his wife’s home, in Sullivan County, New York. (Exhibit D). Finally, as is clear to this Court from the pre-trial conferences concerning bail, the Etkins are not living together and are residing at separate residences. Because the Etkins were “permanently separated,” Etkin cannot invoke the marital communications privilege with respect to the email.²

B. The Email Was Not A Confidential Communication

The defendant’s email to his wife is not and never was a confidential communication. In order to send the email from his work email address, the defendant had to use a New York State Police computer. Each time the defendant used such a computer he was informed – in no uncertain terms – that he had no expectation of privacy while using those computers. Further, as the New York State Police manual concerning emails makes clear – his email to his wife is the property of the New York State Police.

In Wolfe v. United States, 291 U.S. 7, 14 (1934), the Supreme Court held that “wherever a communication, because of its nature or the circumstance under which it was made, was

² In concluding that the Etkins are permanently separated, the Court can also rely on the tenor of and the statements in the emails between the Etkins, submitted by the defendant as an attachment to his affidavit. See In re Witness Before Grand Jury, 791 F.2d at 238 (“either party may bring forward special circumstances that render more or less likely the objective possibility of reconciliation at the time of the communications.”).

obviously not intended to be confidential, it is not a privileged communication.” See In re Witness Before Grand Jury, 791 F.2d at 239 (“Although ‘communications’ between spouses are presumed to be confidential, this presumption is rebutted when the communicant knew that the information was or would be disclosed to third parties or to the public.”) (citations omitted).

Courts considering whether communications between spouses are confidential have focused on the circumstances of the communication. For example, in United States v. Griffin, 440 F.3d 1138 (9th Cir. 2006), the defendant attempted to invoke the marital communications privilege with respect to six boxes of documents – including letters written by the defendant while incarcerated – seized during the search of his wife/attorney’s residence. Id. at 1140. The Ninth Circuit – relying upon California prison regulations that inmate mail “is subject to being read in its entirety or in part by designated employees of the facility before it is mailed for or delivered to an inmate” – held that the defendant “had no right to protect from disclosure to the government as privileged marital communications those portions of his letters to his wife/attorney.” Id. at 1145.

Where courts have concluded that a party should have expected that his or her communication was not private, they have rejected the invocation of the marital communications privilege with respect to that communication. See United States v. Madoch, 149 F.3d 596, 602 (7th Cir. 1998) (rejecting invocation of marital communications privilege because communications from jail are likely to be monitored by prison authorities and overheard by others); United States v. Harrelson, 754 F.2d 1153, 1169-70 (5th Cir. 1985) (no marital communications privilege during prison visit where eavesdropping could reasonably be expected to occur).

The defendant's email to his wife – by way of his official government email account using a New York State Police computer, (Exhibit A at ¶ 4) – cannot be considered confidential. The defendant was specifically informed that he had “no legitimate expectation of privacy” in either his email communications or the use of his official computer. (Exhibit B). Each time the defendant used the computer, he was advised:

For authorized use only. The system and all data are the property of the New York State Police Use of this system is only permitted under the authority of the New York State Police and subject to policies, procedures and acceptable use as outlined in the NYSP Administrative Manual Section 11Q and the NYSP Civilian Employee Manual Section 12D. Any use of the NYSP computer system constitutes express consent for the authorized personnel to monitor, intercept, record, read, copy, access and capture such information for use or disclosure without additional prior notice. Users have no legitimate expectation of privacy during any use of this system or in any data on this system. Your access may be logged at any time.

(Exhibit B). At the end of each “banner” notice, which would appear when the defendant “logged into” or “booted up” the computer, was a sentence informing the defendant that by continuing to use the computer, he consented to these conditions.³

Defendant's argument that his email to his wife is protected by the marital privilege is meritless. The defendant was well aware when he sent the email to his wife that it was not private because: (1) he was on notice that he had no expectation of privacy in his computer use; and (2) he had given express consent to the NYSP – by logging on to NYSP computers – to

³ The two “banner” notices that would appear on each computer differed only in the text of the last sentence. The computer assigned to Etkin had a banner notice that concluded: “By logging into this system, you are agreeing that you have read and accepted the above terms and conditions.” (Exhibit B). The other computer that Etkin would use on occasion stated: “If you DO NOT consent to the above do not continue the boot-up process and refrain from further access.” (Exhibit B).

monitor, read and record his computer use and emails. Further, as set forth in Article 11Q of the NYSP Administrative Manual, emails are the “property of the NYSP,” Article 11Q9(d), and “there is no provision for sending or receiving private or confidential electronic communications.” Article 11Q9(c).⁴ (Exhibit C). Because the defendant’s email to his wife was never private, it is not a confidential communication protected by the marital privilege.

C. Even If The Email Was A Confidential Communication, The Privilege Has Since Been Waived By the Defendant.

Assuming arguendo that the defendant’s email to his wife was a confidential communication at the time of its creation, by printing the email out and carrying it with his investigative files for over six months in a state owned police car and thus exposing the document to potential discovery, the defendant waived the privilege by not keeping the email confidential. The email was not found on the defendant’s computer in his home, but rather among his work related materials in a New York State Police car assigned to the defendant. (Exhibit A at ¶ 3). Rather than keeping the document private, Etkin risked its discovery in such a situation as occurred here. See Houghton v. Wyoming, 526 U.S. 295, 303 (all automobile drivers “possess a reduced expectation of privacy with regard to the property that they transport in cars, which travel through public thoroughfares, seldom serve as the repository of personal effects, are subjected to police stop and examination to enforce pervasive governmental controls as an

⁴ As in Griffin, where the defendant there improperly used the prison mail by sending personal communications to his wife under the cover of “attorney mail,” the defendant’s use of his official email account was not authorized under the NYSP Administrative Manual. The NYSP E-mail policy states that: “Personnel may use New York State Police computer equipment to communicate via E-Mail outside of the Division when such communications are related to legitimate business activities and are within their professionally-related job assignments or responsibilities.” (Exhibit C, Article 11Q9(b)) .

everyday occurrence, and, finally are exposed to traffic accidents that may render all their contents open to public scrutiny”) (internal quotation marks and citations omitted).

Further, any claim that the email was privileged was forever lost when the defendant and his counsel filed the email with the Clerk of the Court and thus placed the email into the official court record allowing anyone to view the emails and their contents. “[P]rivileged documents . . . are not protected if a party voluntarily discloses them.” United States v. Gangi, 1 F. Supp. 2d 256, 263 (S.D.N.Y. 1998). As the Court in Gangi stated: “If a party voluntarily discloses a privileged document, it waives the privilege for that document and cannot later seek to keep the document confidential.” Id. (citations omitted).⁵ By filing the email with the Clerk of the Court without taking any measure to protect it from public view, the defendant cannot now claim that the email is confidential and privileged. Even if the document was once confidential, the email lost all its confidentiality when it was docketed in the court file.

Finally, if the defendant did not waive the privilege by publicly filing the email with the Court so that any member of the public could view the email, the defendant’s delay in seeking a judicial determination with regard to the document waived the privilege. At least one Court of Appeals has found that – in the context of the attorney-client privilege – a defendant may waive the privilege with regard to privileged documents if his counsel, as here, waits a considerable period of time between discovering the Government’s possession of allegedly privileged documents and filing a motion seeking relief from the Court. In In re Grand Jury (Impounded),

⁵ Any claim that the disclosure of the email was “inadvertent” would be meritless. In Etkin’s Affirmation – also filed with the Court, Etkin states: “On or about March 13, 2007, I printed Bess’s email to me that contained my earlier email to her. (Attached is a copy of the email).” (Etkin Aff. ¶ 3). Both Etkin and counsel knowingly filed the email with the Court.

138 F.3d 978 (3rd Cir. 1998), the Third Circuit held that the district court did not abuse its discretion in holding that an individual “waived the privilege . . . in waiting nearly four months to seek a judicial vindication of his assertion of the privilege.” *Id.* at 982. The Third Circuit held that an attorney’s letter to the Government eight days after a file was seized asserting attorney-client privilege and “repeated admonitions to [the Government] to return the protected documents,” *id.*, was not sufficient because it is incumbent upon counsel to “seek a judicial determination of the controversy if his or her adversary took an opposing stance.” *Id.* The Third Circuit concluded that

Merely asserting the privilege to an adversary is not sufficient to protect the privilege . . . inasmuch as the adversary has possession of the documents and thus can make use of them Judicial enforcement of the privilege was the only remedy that [the individual] could have obtained which would have foreclosed the United States from further use of the seized file. Without such judicial vindication, the United States was free to continue to utilize the documents, thereby negating their confidential nature.

Id. Here, the email was recovered from the car on September 28, 2007. Counsel was provided with a copy of the email (along with other documents recovered from the car) on October 12th, but counsel waited until December 10th to file his motion seeking dismissal of the Indictment. By waiting approximately two months to seek a judicial resolution with regard to the email, counsel has further waived any possible claim that the document is privileged.

II.

IF THE COURT CONCLUDES THAT THE EMAIL IS PRIVILEGED, DEFENDANT IS ENTITLED ONLY TO SUPPRESSION OF THE EMAIL

Baldly arguing that the Government’s review of the email has prejudiced the defendant, counsel seeks dismissal of the indictment, or in the alternative, a hearing pursuant to *Kastigar v.*

United States, 406 U.S. 441 (1972), at which the Government would be required to establish that its evidence is free from “taint and that the further prosecution of defendant by the current prosecution team is proceeding wholly independent of anything learned from being exposed to privileged material.” (Br. 5). The defendant, however, would not be entitled to either of these extraordinary forms of relief. Rather, at most, the defendant would be entitled to suppression of any evidence that he demonstrates to contain confidential marital communications.

A. There is No Support In Case Law For Counsel’s Argument That A Breach Of The Marital Privilege Should Be Governed By Reference To The Law Governing Attorney-Client Privilege

Counsel argues in a conclusory fashion, without any support in case law, that the “fact that the privilege at issue in this motion is the marital privilege [rather than the attorney-client privilege] does not change the analysis.” (Etkin Mem. 4 n.1). The defendant is unable to cite: (1) any case involving a violation of the marital privilege in which an Indictment was dismissed;⁶ (2) any case involving the marital privilege in which a “taint hearing” has been held;⁷ (3) any case in

⁶ Contrary to the defendant’s claim, this is not a case where the Government “intentionally intruded into the marital privilege ‘domain.’” (Br. 7). Nor, is there any basis to dismiss the Indictment based upon the Government’s conduct. Further, even the case law cited by the defendant makes clear that the Second Circuit “has never adopted the per se rule of dismissal [of an indictment].” United States v. Gartner, 518 F.2d 633, 637 (2d Cir.1975) (discussing that the per se rule is a unique sanction applying to only the most grave of violations including intentionally planting a government investigator in the defense camp, trying a “dummy” defendant with other co-defendants, and intentionally intercepting phone calls between a defendant and her attorney) (citations omitted).

⁷ Nor, could the defendant ever establish any “taint” or prejudice. The Government has stated that the crime discussed in the email is not direct evidence of the crime charged in the Indictment, but rather “other act” evidence subject to Fed. R. Evid. 404(b).

which a “firewall” was used with respect to allegedly privileged marital communications;⁸ and (4) any case in which the prosecution team was disqualified from the prosecution after being exposed to a marital communication.⁹

⁸ The reason is quite clear – the case law that the defendant relies upon exclusively deals with cases in which the Government is searching the office of an attorney or speaking to an attorney who had represented the defendant – an instance in which the Government is well aware in advance that there is the distinct possibility of discovering potentially privileged material. Searches of houses occupied by married individuals occur everyday in this country without law enforcement utilizing a “taint” team to search the house and initially review the evidence. Here, the email was not even recovered from the defendant’s house, but rather from a bag – inside his official car – which contained investigative material belonging to an official government agency.

Any breach of the marital privilege in this case, assuming there was one, was inadvertent. Here, after reading the email at least a couple of times, Agent Miller came to the conclusion that the email was not only a communication between the defendant and his wife, but also a statement about a crime – a crime in which an individual could have been unjustly incarcerated.

Moreover, the defendant’s argument that the “communications should not have been reviewed by the Government” is nonsensical. (Br. 3). To the extent that the defendant is arguing that the Government must return a document without ascertaining its nature or making a determination as to whether or not it is privileged solely because it is a communication between a husband and wife, that argument has no basis in law. Further, to even suggest that FBI agents should be aware of a crime where someone may have been improperly incarcerated and not to seek to investigate the circumstances is ludicrous.

Finally, the defendant essentially argues that there is no method by which the Government could have safely reviewed the communication. While advocating a firewall in one section of his brief, the defendant concomitantly contends that such a method has been “disapproved” by three judges of this Court. (Compare Br. 4 with Br. 4 n.2). Interestingly, on October 12, 2007, the defendant, in the presence of his attorney, consented to a search of a computer hard drive and other electronic media found in the defendant’s official NYSP car. At no point has defense counsel requested or inquired as to whether a “firewall” was in place to review any materials that would be recovered from those media.

⁹ The cases cited by the defendant – in the attorney-client context – as providing a basis to disqualify the prosecution team are by no means similar to the circumstances here. See United States v. Horn, 811 F. Supp. 739 (D. N.H. 1992) (removing prosecutor because, among other reasons, prosecutor intentionally sought to learn defense trial strategy by having copier company make a second set of the documents the defense team sought to have copied, reviewing documents in defiance of a court order and demonstrating a lack of candor with the district

The case law concerning the marital privilege makes clear that the privilege is not constitutionally grounded, and as a result, it is not subject even to a “taint” or “fruit of the poisonous tree” analysis. See United States v. Marashi, 913 F.2d 724, 731 n. 11 (9th Cir.1990) (holding in a case concerning the marital communications privilege that “no court has ever applied [the ‘fruits of the poisonous tree’] theory to any evidentiary privilege and . . . we have indicated we would not be the first to do so”); United States v. Lefkowitz, 618 F.2d 1313, 1318 n. 8 (9th Cir.1980) (“Because we reject . . . Lefkowitz’s argument that the marital privileges are somehow constitutionally grounded in, among other locations, the Fourth Amendment, we doubt that a secondary source of information obtained through information protected by the confidential marital communications privilege would in any way be ‘tainted.’”).

The reason why counsel is unable to identify any law supporting his argument should be clear from the nature of the privileges. The marital privilege is concerned with the “promot[ion] [of the] marriage,” Vo, 413 F.3d at 1016, while the attorney-client privilege serves to ensure that the opposing adversary does not obtain access to information concerning trial strategy and effective representation of the client – information that once obtained could forever prejudice counsel’s defense of the client.

Notwithstanding the lack of any law concerning the marital privilege to support the defendant’s argument that he is entitled to the vast relief that he seeks, as the Government argues infra, even the law concerning the attorney-client privilege makes clear that his argument is

court); United States v. (Under Seal), 757 F.2d 600 (4th Cir. 1985) (holding that government’s challenge to a disqualification order – imposed by the district court after prosecutor had reviewed files that the district court had determined were privileged – was moot and concluding that sanction of dismissal of the indictment was not appropriate).

meritless.

B. There Is No Basis To Dismiss The Indictment

The Supreme Court has held that “an indictment valid on its face is not subject to challenge on the ground that the grand jury acted on the basis of inadequate or incompetent evidence, . . . or even on the basis of information obtained in violation of a defendant’s Fifth Amendment privilege against self-incrimination. United States v. Calandra, 414 U.S. 338, 344 (1974) (citations omitted); see also United States v. Williams, 504 U.S. 36, 49 (1992) (citing examples of constitutional protections usually afforded criminal defendants that have no application in the grand jury setting); United States v. Blue, 384 U.S. 251, 255 (1966) (“Even if we assume that the Government did acquire incriminating evidence in violation of the Fifth Amendment, Blue would at most be entitled to suppress the evidence and its fruits if they were sought to be used against him at trial.”).

Construing these precedents, the Second Circuit has held with regard to the attorney-client privilege, that even if the Government presents material subject to the attorney-client privilege in a grand jury proceeding, it provides no basis for dismissing an indictment. United States v. Bein, 728 F.2d 107, 113 (2d Cir. 1984) (“[C]ourts have declined to dismiss indictments because of the use of privileged matter before the grand jury . . . including testimony by attorneys as to privileged communications, the precise issue before us.”); accord United States v. Haynes, 216 F.3d 789, 797-98 (9th Cir. 2000); United States v. Wolfson, 558 F.2d 59, 66 n. 22 (2d Cir. 1977); United States v. Colasurdo, 453 F.2d 585, 595-96 (2d Cir. 1971). If presentation of evidence violative of the attorney-client privilege does not merit dismissal of an indictment, surely neither would an infringement of the marital communications privilege.

In any event, there is no claim in this case that the Government presented privileged material to the grand jury nor could there be. The grand jury returned the Indictment against the defendant the day before he was arrested and the email was recovered during a search of his official police car. As a result, any argument that the Indictment should be dismissed is meritless.

C. The Defendant Is Not Entitled To A Kastigar Hearing

The defendant makes no claim that the Government intentionally obtained information allegedly subject to the marital communications privilege.¹⁰ Assuming arguendo that the email is privileged, it could not be offered in evidence at trial over Etkin's objection. But the Government's receipt of that document does not presumptively taint all of its other evidence and the agents and prosecutor who viewed it.¹¹ If that were so, federal prosecutions would be subject

¹⁰ Throughout his brief, counsel seeks to confuse the important distinction between intentionally obtaining material, e.g. executing a search warrant in an attorney's office or intercepting conversations that it knows are occurring between an attorney and his client, and reviewing material lawfully obtained during a search of the defendant's official car. Here, as set forth in Agent Presutti's affidavit, Agent Miller was reviewing material found in the bag as part of an inventory search of the car and to identify materials that would have to be returned to either the Sullivan County Sheriff's Department. (Exhibit A at ¶ 3).

¹¹ The case law concerning claims of "taint" is an extension of the Exclusionary Rule established in Weeks v. United States, 232 U.S. 383 (1914) and Mapp v. Ohio, 367 U.S. 643 (1961), and the bar on using "fruits" of suppressed evidence established in Silverthorne Lumber Co. v. United States, 251 U.S. 385, 391-92 (1920) and Wong Sun v. United States, 371 U.S. 471, 488 (1963), which has developed principally in cases in which illegal wiretaps had been identified as a possible source of evidence used to convict defendants. See, e.g., Alderman v. United States, 394 U.S. 165 (1969); Nardone v. United States, 308 U.S. 338 (1939). Defendants have also raised claims of "taint" where unconstitutional searches and seizures have occurred in an effort to suppress evidence derived from those searches. See, e.g., United States v. Birrell, 269 F. Supp. 716 (S.D.N.Y. 1967) (seeking a "taint" hearing where a search warrant lacking in sufficient supporting probable cause had been executed). Generally, defendants raising "taint" claims seek hearings at which the Government may be required to demonstrate that the evidence and testimony used to convict a defendant was not improperly derived from

to a Kastigar bar every time Government agents obtained any privileged document or information in the course of their investigation. Moreover, breaches of common-law evidentiary privilege which the Supreme Court has many times emphasized should be strictly construed – would result in broader suppression than intentional violations of constitutional rights.

In Kastigar v. United States, 460 U.S. 441 (1972), the Supreme Court prescribed the Fifth Amendment protections that apply when the Government seeks to prosecute an individual after compelling his testimony through a grant of immunity. In such circumstances, the Supreme Court held, the prosecution has the duty to prove “that the evidence it proposes to use is derived from a legitimate source wholly independent of the compelled testimony.” 406 U.S. at 460. This

suppressed evidence.

It is well established that the proponent of a “taint” claim bears the burden of going forward. Under Nardone and its progeny, a defendant must first prove that a constitutional violation occurred, and then must be given an opportunity, “however closely confined, . . . to prove that a substantial portion of the case against him was a fruit of the poisonous tree.” Nardone, 308 U.S. at 341 (emphasis supplied); Alderman, 394 U.S. at 183 (quoting Nardone); see United States v. Mullen, 451 F. Supp. 2d 509, 540 (W.D.N.Y. 2006) (“The proponent of a taint hearing has the initial burden of ‘producing specific evidence demonstrating taint in a substantial portion of the Government’s case against him.’” (emphasis supplied) (quoting United States v. Sapere, 531 F.2d 63, 66 (2d Cir. 1966)) (citing Alderman, 394 U.S. at 183)); United States v. Sacco, 563 F.2d 552, 558 (2d Cir. 1977) (in post-trial motion, defendant utterly failed to meet his “initial burden of producing specific evidence demonstrating taint in a substantial portion of the Government’s case against him” where no evidence was presented to the district court apart from the mere existence of the wiretaps) (emphasis supplied); see also United States v. Apple, 915 F.2d 899, 906 (4th Cir. 1990) (claimant has the initial burden of coming forward with specific evidence demonstrating taint). Only after defendant meets that high burden may the Government be put to the test of convincing the trial court “that its proof had an independent origin.” Nardone, 308 U.S. at 341; Alderman, 394 U.S. at 183 (quoting Nardone); see Wong Sun, 371 U.S. at 487-88 (“We need not hold that all evidence is fruit of the poisonous tree simply because it would not have come to light but for the illegal actions of the police. Rather the more apt question in such a case is whether, granting the establishment of the primary illegality, the evidence to which instant objection is made has been come at by exploitation of that illegality or instead by means sufficiently distinguishable to be purged of the primary taint.”) (emphasis supplied).

protection is necessary, the Supreme Court emphasized, because the scope of immunity flowing from the Government's compulsion must be "coextensive with the scope of the privilege [against self-incrimination]," Id. at 441, and calculated to place the defendant "in substantially the same position as if the witness had claimed his privilege in the absence of a state grant of immunity." Id. at 457 (internal quotation marks and citation omitted).

The Kastigar standard is more stringent than the "fruit of the poison tree" standard generally applied when the Government obtains evidence in violation of the defendant's constitutional rights. See United States v. Kurzer, 534 F.2d 511, 516 (2d Cir. 1976) (discussing distinctions between Kastigar and "fruit of the poison tree" analysis). Under the fruit of the poison tree analysis, "[a] mere causal connection between information gained during an illegal search and evidence prepared for trial does not require automatic exclusion of the evidence." United States v. Watson, 950 F.2d 505, 507 (8th Cir. 1991). Nor is suppression warranted merely because "the evidence would not have been discovered 'but for' the illegal conduct." Id.

Numerous cases have addressed the question of what standard should apply when the Government comes into possession of information subject to the attorney-client privilege or other common-law evidentiary privileges. All have rejected the Kastigar standard. Indeed, all have rejected even the less stringent "fruit of the poison tree" analysis. The issue was most recently and thoroughly addressed in United States v. Squillacote, 221 F.3d 542 (4th Cir. 2000). There, FBI agents intercepted and transcribed conversations between the defendant and her psychologist that were later determined to be privileged. As a result, the defendant requested a hearing under Kastigar to require the Government to prove that the evidence it would present at trial was derived from sources independent of the privileged communications. Id. at 558. The district

court refused to hold the hearing, however, concluding that such a hearing was required only when a constitutionally-based privilege was at issue. *Id.* The Fourth Circuit agreed with the district court, holding that no hearing was required and that the defendant was not entitled to suppress any of the derivative fruits of the privileged communication. *Id.* at 560.

The Fourth Circuit specifically ruled that “Kastigar analysis is not triggered by the existence of evidence protected by a privilege, but instead by the government's effort to compel a witness to testify over the witness’ claim of privilege.” *Id.* at 559. In so ruling, the court stressed that Kastigar was intended to enforce a “total prohibition on use” arising from the Fifth Amendment and that the Supreme Court had “‘particularly emphasized the critical importance of protection against a future prosecution based on knowledge and sources of information obtained from the compelled testimony.’” *Id.* (emphasis in original) (quoting United States v. Hubbell, 530 U.S. 27, 39 (2000)). The court reasoned that, “because the government's right to compel testimony in the face of a claim of privilege is the issue at the heart of Kastigar, its protections do not apply in cases where there is privileged evidence, but no compelled testimony.” *Id.* at 560. The court also stressed that common-law evidentiary privileges and constitutional protections were not analogous, noting that evidentiary privileges were required to be “‘strictly construed.’” *Id.* (quoting Trammel v. United States, 445 U.S. 40, 50 (1980)).

The Tenth Circuit reached similar conclusions in Nickel v. Hannigan, 97 F.3d 403 (10th Cir.1996). Nickel squarely presented the issue of whether the Government can make “derivative use” of information obtained in breach of the attorney-client privilege. The appellant confessed committing a murder to his attorney. In breach of the privilege, the attorney then communicated this confession to the police, leading to the appellant’s arrest and subsequent confession to the

police. Id. at 405. At the appellant's murder trial, the attorney was called as a witness to the initial confession. Id. at 406. The Tenth Circuit held that the testimony of the attorney would have been suppressed if a proper objection had been made. It, however, held that the derivative fruits of the appellant's privileged communications with the attorney were not subject to suppression. Id. at 409. The Tenth Circuit stressed that "other courts have refused to apply such a broad evidentiary rule of exclusion to breaches of [the attorney-client] privilege" and that it too would decline to do so in the absence of contrary state law. Id. As a result, the Tenth Circuit concluded that the appellant was not entitled to suppress any proof other than the confession to the attorney.

All of these cases recognize a distinction between the policies served by the Fifth Amendment and other constitutional rights and the policies served by common-law privileges. They also implicitly recognize important practical concerns. As many of the cases illustrate, the Government often cannot avoid exposure to privileged material. In the course of searches, interviews, wire taps, grand jury questioning, and other investigative activity, agents and prosecutors are frequently exposed, in some manner or degree, to documents or information subject to a potential claim of privilege. In contrast, the Government controls the decision to immunize testimony and makes a considered choice when it does so. If the stringent protections of Kastigar were applied every time members of a prosecution team were exposed to any privileged matter, prosecutions would be terminated without any important, countervailing interest being served.

D. Neither Schwimmer Nor Weissman Make Clear That “Derivative Use” Of Privileged Material Is Prohibited.

There is some authority in the Second Circuit for the proposition that the attorney-client privilege bars use not only of privileged communications but evidence “derived from” privileged communications. In United States v. Schwimmer, 892 F.2d 237 (2d Cir. 1989), the Second Circuit held that the Government had elicited in grand jury proceedings privileged testimony and analysis of an accountant who had been hired to perform analysis on behalf of defense attorneys. Although the Government asserted on appeal that all of this information was capable of being obtained from other sources, the Second Circuit found that “[t]here is reason to question that assertion” based on the nature of the accountant work papers that were furnished to the Government. Id. at 245. Accordingly, the Second Circuit found that, “based on the documentation available to it, the district court should have conducted an evidentiary hearing to determine whether the government’s case was in any respect derived from a violation of the attorney-client privilege.” Id. The Second Circuit, however, remanded the case without any direction as to the standard that should be applied or where the burden of proof rested.

On remand, the district court refrained from deciding these questions because it concluded that the Government had demonstrated a lack of taint even measured by the Kastigar standard. United States v. Schwimmer, 738 F. Supp. 654, 658 (E.D.N.Y. 1990) (McLaughlin, J.) (“Because I conclude that the government has satisfied the “heavy burden” described in Kastigar, I may assume, without deciding, that the defendant’s contention is correct [as to the applicability of that standard].”), aff’d, 924 F.2d 443 (1991). On appeal of the district court’s ruling, the Second Circuit also had no need to decide these questions. Like the district court,

however, it assumed the applicability of the Kastigar standard and upheld the district court's finding that the Government had met that standard, noting that the finding was "amply supported by evidence produced at the hearing" and "not clearly erroneous." United States v. Schwimmer, 924 F.2d 443, 446 (2d Cir. 1991).

In United States v. Weissman, 1996 WL 751386 (S.D.N.Y. Dec. 26, 1996), Judge Haight did much the same thing as the district court and Second Circuit in Schwimmer: assuming the applicability of Kastigar and rejecting a claim of taint under that standard. See 1996 WL 751386, *9-10. Judge Haight went one step further, however, noting that he saw "no principled distinction" between the situation in which the Government receives materials subject to attorney-client privilege and the situation in which it compels testimony over the defendant's Fifth Amendment objection. Id. at *10.

Neither Schwimmer nor Weissman, therefore, had occasion to decide which party bears the burden of proving taint or lack of taint and what type of "derivative use" of privileged material is prohibited. To the extent that dicta in those cases suggests that Kastigar prescribes these standards, the dicta is inconsistent with all the decisions outside this Circuit that have squarely addressed these questions, with other statements in Schwimmer itself, and with other decisions of the Second Circuit.

For example, the Schwimmer court itself stressed that "unless 'the conduct of the Government has . . . been . . . manifestly and avowedly corrupt,'" a defendant seeking dismissal of convictions based on governmental use of privileged information "must show prejudice to his case resulting from the intentional invasion of the attorney-client privilege." Schwimmer, 924 F.3d at 447 (quoting United States v. Gartner, 518 F.2d 633, 637 (2d Cir. 1975)). That

requirement, however, cannot be squared with application of Kastigar in circumstances in which breach of the privilege is unintentional. For the burden of proof on the issues of taint and prejudice cannot logically rest with the defendant when the Government intentionally intrudes on the privilege and shift to the Government when the breach is unintentional.

Numerous other cases, moreover, make clear that the Second Circuit does not contemplate that a hearing under the standards triggered by compelled testimony is required every time the Government is exposed to privileged material in the course of investigation. In United States v. Colasurdo, for example, attorneys for the defendants were interviewed by the United States Attorney's office and testified before the grand jury. Claiming breach of the privilege in these communications, the defendants argued on appeal of their convictions that the district court should have dismissed the charges based on disclosure of privileged information to the grand jury. In rejecting this claim, Judge Friendly stressed that, if defendants could claim a right to dismiss charges on this basis, "before trial on the merits there would always be a kind of preliminary trial to determine the competency and adequacy of the evidence before the grand jury, with resultant delay." 453 F.2d at 595. The Second Circuit reaffirmed this ruling in United States v. Bein, 728 F.2d at 113.

Although the claims in Colasurdo and Bein were directed at evidence used in the grand jury, Judge Friendly's concern about avoiding "preliminary trials" would equally apply to the hearing that the defendant requests here. For the defendant argues that every instance in which privileged information is disclosed to the Government triggers a Kastigar hearing at which the Government must essentially prove that all its evidence is untainted. Under the defendant's argument, the convictions in Colasurdo and Bein could not have been sustained without a

hearing in which the Government demonstrated that all of its trial proof derived from sources wholly independent of the privileged information allegedly disclosed or used in connection with grand jury proceedings. Yet neither decision required such a hearing. Nor did either decision suggest that such a hearing would be required if the appellants had styled their arguments differently.

Under these authorities, the pretrial disclosure of privileged communications, without more, does not trigger the right to a hearing, much less shift the burden of proving lack of prejudice to the Government. These authorities make clear that the Second Circuit, – like other courts that have squarely addressed the issue – has not concluded that a breach of an evidentiary privilege triggers the special protections that Kastigar held to be applicable when the Government seeks to prosecute a defendant after compelling his testimony by grant of immunity. Rather, the defendant would be entitled, at most, to suppress the communication and any evidence that directly or indirectly incorporates privileged material.

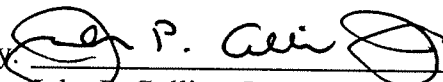
CONCLUSION

For the foregoing reasons, defendant's motion to suppress the email and for a pretrial "taint" hearing should be denied without a hearing.

Dated: January 7, 2008
White Plains, New York

Respectfully submitted,

MICHAEL J. GARCIA,
United States Attorney for the
Southern District of New York,
Attorney for the United States of America

By: 

John P. Collins, Jr.
Assistant United States Attorney
(914) 993-1919

AFFIRMATION OF SERVICE

JOHN P. COLLINS, JR., pursuant to Title 28, United States Code, Section 1746, hereby declares under penalty of perjury that:

On January 7, 2008, I served one copy of the within Government's Memorandum of Law in Opposition to Defendant's Motion to Preclude the Government from Introducing into Evidence an Email Sent by the Defendant to His Wife and For a Taint Hearing by causing the same to be enclosed in a Federal Express envelope addressed to:

Kerry A. Lawrence, Esq.
Briccetti, Calhoun & Lawrence, LLP
81 Main Street, Suite 450
White Plains, NY 10601

and causing the envelope to be placed in the outgoing mail for Federal Express delivery from 300 Quaroppas Street, White Plains, New York 10601.

Executed on January 7, 2008, at White Plains, New York.



JOHN P. COLLINS, JR.
Assistant United States Attorney
Tel. No.: (914) 993-1919

EXHIBIT A

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----	x	
	:	
UNITED STATES OF AMERICA	:	
	:	
- v -	:	
	:	07 Cr. 913 (KMK)
PHILIP ETKIN,	:	
	:	
	:	
Defendants.	:	
	:	
-----	x	
STATE OF NEW YORK)	
COUNTY OF ORANGE	: ss.:	
SOUTHERN DISTRICT OF NEW YORK)	

VINCENT PRESUTTI, pursuant to Title 28, United States Code, Section 1746,
hereby declares:

1. I am employed as a Special Agent with the Federal Bureau of Investigation ("FBI") and am the case agent for the investigation and prosecution of Philip Etkin.
2. In or about September 2007, during the course of my investigation, I spoke to Art Hawker, the Chief of Patrol for the Sullivan County Sheriff's Department about Philip Etkin. During the course of my discussions, Hawker informed me, in sum and substance, that it was his understanding – based upon a prior conversation with one of Etkin's colleagues – that Etkin had been separated from his wife for approximately one year.
3. On September 28, 2007, I, and other agents, arrested Philip Etkin. At the time of his arrest, Etkin was driving a vehicle that belonged to the New York State Police ("NYSP") and had been assigned to Etkin because of his status as a cross-designated police officer. Prior to his arrest, the Sullivan County Sheriff's Office had asked the FBI to return to the Sullivan County Sheriff's Office any case files or materials relating to investigations involving

the Sullivan County Sheriff's Office and the NYSP Mid Hudson Drug Task Force (to which Etkin was assigned). I have spoken to one of the agents – Special Agent Jessica Miller – who participated in the search of the car that day and Agent Miller has told me, in sum and substance, that: (1) She participated in an inventory search of the car; (2) While searching the passenger area of the car, she saw an open portfolio bag on the front passenger seat of the car; (3) She saw that inside the portfolio bag were file folders; (4) She began looking through the file folders and saw in the file folders what appeared to be investigative materials – including Department of Motor Vehicle and license plate information – and notes; (5) In addition to investigative materials and notes, she also observed Sullivan County PBA materials in at least one of the folders; (6) In one of the file folders was an email; (7) After reading the email at least a couple of times, she then concluded that the email correspondence was between Etkin and his wife and that the email correspondence contained information concerning a crime; and (8) Thereafter, she showed the email to me and it was later placed in evidence.

4. In or about December 2007, I contacted Inspector Mark Smith, who is a Staff Inspector with the Internal Affairs Division of the NYSP. Inspector Smith has informed me, in sum and substance, that in or about January 2007, Etkin became a cross designated police officer and was assigned to a NYSP Multi-Jurisdictional Task Force. Because Etkin was a cross-designated police officer assigned to a NYSP task force, the NYSP assigned him various items including: (1) a NYSP Division Vehicle; (2) a NYSP Nextel cellular telephone; and (3) a NYSP laptop computer. According to Inspector Smith: (1) Etkin was also assigned a NYSP email address: petkin@troopers.state.ny.us; and (2) in order to access that NYSP email account, Etkin

would have to use a NYSP computer because he was not authorized to access his NYSP email account from a home computer.

5. Inspector Smith also provided me with an email documenting the NYSP computers that Etkin used and the notices that would appear when Etkin would "log on" or "boot up" each computer. That email is attached as Exhibit B. According to Inspector Smith, as a cross-designated police officer, Etkin was subject to the regulations in the NYSP Administrative Manual. Inspector Smith provided me with a copy of NYSP Administrative Manual Section 11Q (Information Technology). Section 11Q is attached as Exhibit C.

6. I declare under penalty of perjury that the foregoing is true and correct, pursuant to Title 28, United States Code, Section 1746.

Dated: Goshen, New York
January 7, 2008



Vincent Presutti
Special Agent
Federal Bureau of Investigation

EXHIBIT B

From: Scott Wilcox
To: Smith, Mark
Date: 12/12/2007 12:37:57 PM
Subject: Re: Fwd: Etkin computer

Inspector,

This is the text of the banner that appears on the computer that was assigned to Etkin (Ser. #8V73S91).

Notice:

For authorized use only. This system and all data are the property of the New York State Police. Unauthorized use or attempted unauthorized use of this system by persons not issued a user account is not permitted and may constitute a state or federal offense.

Use of this system is only permitted under the authority of the New York State Police and subject to policies, procedures and acceptable uses as outlined in the NYSP Administrative Manual Section 11Q and the NYSP Civilian Employee Manual section 12D. Any use of the NYSP computer systems constitutes express consent for the authorized personnel to monitor, intercept, record, read, copy, access and capture such information for use or disclosure without additional prior notice. Users have no legitimate expectation of privacy during any use of this system or in any data on this system. Your access may be logged at any time.

By logging into this system, you are agreeing that you have read, and accepted the above terms and conditions.

The one he would use occasionally (Ser. #BC6J141) would display this banner:

FOR AUTHORIZED USE ONLY. This system and all data are the property of the New York State Police. Unauthorized use or attempted unauthorized use of this system by persons not issued a user account is not permitted and may constitute a state or federal offense. Use of this system is only permitted under the authority of the New York State Police and subject to the policies, procedures and acceptable use as outlined in the NYSP Administrative Manual and NYSP Civilian Manual. Any use of NYSP computer systems constitutes express consent for authorized personnel to monitor, intercept, record, read, copy access and capture such information for use or disclosure without additional prior notice. Users have no legitimate expectation of privacy during any use of this system or in any data on this system. Your access may be logged at any time. If you DO NOT consent to the above do not continue the boot-up process and refrain from further access.

>>> Mark Smith 12/12/2007 11:18 AM >>>

>>> Mark Smith 12/12/2007 10:57:37 AM >>>
These were the computers that the target would use

>>> Brendan Casey 12/12/2007 10:48:24 AM >>>
Insp, these are the computers Phil had access to

Lt. Brendan R. Casey
Hudson Valley
CNET - MHDETf - GIU
Office
Cell - **REDACTED**

>>> Ethan Fergus 12/12/2007 10:33 AM >>>

>>> Joseph Candela 12/12/2007 10:27 AM >>>
E,

Phil had the following laptops assigned to him during the stated time periods.

- 1) from 1/07 to 3/2/07 Property Tag #PCSU032303 Ser. #6RJLQ31.
- 2) from 3/2/07 to his dismissal Property Tag #ISL70078 Ser. #8V73S91.

3) The CPU in Otis's office. Phil would use on occasion: Ser. #BC6J141.

Joe

EXHIBIT C

NYSP Administrative Manual - Article 11

[10 04-08 7/04]

- (b) If a current MSDS is already on file for a specific product, from the same manufacturer it is not necessary to request another one.
 - (c) If products are mixed by Members or Employees and subsequently stored in another container, the container must be labeled with regard to:
 - (1) Product name;
 - (2) Name and address of manufacturer;
 - (3) Identity of hazardous materials contained therein;
 - (4) Physical and health hazards possible if exposure limits are exceeded; and
 - (5) Any internal organs that may be directly effected by exposure to the hazardous material.
- It is not necessary to label secondary containers when the same Employee pours the mixture, maintains continuous custody, and either pours the substance back into the original container or properly disposes of the substance.

11Q INFORMATION TECHNOLOGY**11Q1 Information Technology**

To improve the efficiency and effectiveness of our operations, the State Police utilizes a variety of information technology tools and equipment including desktop and laptop (portable) computers, data communication networks, data and application servers and an array of commercial and internally developed software and applications. All hardware, software and data components are to be used only for official business and are to be managed as directed by the Division.

Each Troop, Detail or Section shall continue the current policy of assigning a PC Coordinator to coordinate all information technology activities, including requests for equipment, maintenance and support and installation and use.

11Q2 Acquisition Of Division Computer Equipment

[CROSS REFERENCE: Article 3 - Supplies, Equipment And Uniform Clothing, Section titled: Inventories.]

- ▣ (a) The acquisition of ALL computer hardware, software and peripheral equipment, including donated equipment, must be approved at the Division level. Property numbers for technology equipment will be issued by Information Services at Division Headquarters.
- (b) All requests for new or replacement computer equipment are to be submitted through Channels to the Troop or Detail Commander, ATTN: PC Coordinator. Requests that are approved at the local level will be forwarded to the Information Services Section.
- (c) Information Services will determine if the request:
 - (1) Is consistent with Division's technology strategy;
 - (2) Meets Division standards; and
 - (3) Can be accommodated from available funds.
- ▣ (d) Upon approval, the items will be ordered and delivery and installation will be scheduled by the Senior Stores Clerk, PC Coordinator and/or Information Services.

- ▣ (e) The purchase of, acquisition and/or implementation of non-standard hardware from outside sources to be used with any of Division's computer systems, networks or communications systems, requires approval from the Information Security Unit.

 - ▣ (1) Prepare and submit a memorandum requesting to install and/or implement non-standard hardware for use with Division technology equipment to the Information Security Unit at Division Headquarters and forward a copy of the request to your PC Coordinator.
 - ▣ (2) The request must justify the need and intended use of the hardware.
 - ▣ (3) If approval is granted, the PC Coordinator or Information Services will arrange for installation of the hardware. A property tag must be affixed to the equipment and the appropriate information recorded in the Technology Information Management (TIM) system.
[CROSS REFERENCE: Article 3 - Supplies, Equipment And Uniform Clothing, Section titled: Inventories.]
- (f) Computer Modems shall not be installed or used in conjunction with Division computer equipment or communications systems without prior written approval from the Information Security Unit. In cases where modems have previously been installed or used, written approval is also required as prescribed below.

 - (1) Employee Requesting Approval:

 - Complete a NYSP Modem Installation/Use Request form (form EDP-3) fully documenting the need for modem use.
 - Forward the completed request form to your Troop/Detail Commander or Section Head.
 - (2) Troop/Detail Commander Or Section Head

 - If you concur with the stated need, endorse the EDP-3 form and forward it to the Information Security Unit at Division Headquarters for review and specific Instructions/requirements.
- ▣ (g) PC equipment will not be reassigned, relocated, connected to or disconnected from the network, without the approval of the PC Coordinator and/or Information Services and proper notification of the Senior Stores Clerk.
- ▣ (h) Software installations will not be changed without the approval of the PC Coordinator and/or Information Services.

 - ▣ (1) Contact your PC Coordinator to request any change in your computer, software or network connection.
 - ▣ (2) If the request complies with subsection (c) above, the PC Coordinator will handle the change in status by contacting the Information Services Section at Division Headquarters.
 - ▣ • PC Coordinator: If you require assistance in completing the request, contact the Information Services Help Desk.

NYSP Administrative Manual - Article 11

[IO 04-08 7/04]

11Q3 Inventory And Audit

- ☐ (a) Inventory of Technology Equipment shall be conducted in the same manner as non-technology equipment. No additions, transfers or disposals shall be made to a Division Installation's Technology Equipment Inventory listing without the approval of the First Sergeant and notification to the Division Quartermaster in writing by submission of a Technology Equipment Addition, Transfer Or Disposal Record (form QM-26T).
- ☐ (b) As part of the internal inspection process of Division facilities, PC hardware and software shall be checked against the master technology inventory listing. The technology inventory listing may be obtained at Troop level from the PC Coordinator or Senior Stores Clerk, or from the Information Services Section at Division Headquarters.

11Q4 Assignment Of PC Equipment

- (a) All PC Equipment is assigned to a Troop, Detail or Section. Exception: Laptop computers are issued to Field BCI Investigators and are an accountable item. The laptop computer will remain with the Field BCI Investigator during his/her tenure as such and will be turned in when he/she is promoted or appointed to a different rank, transferred to a non-Field position, or is separated from Division service. When separated from Division service, the laptop computer will be turned in with other BCI-issued equipment.
- (b) Division Quartermaster And/Or Troop Senior Stores Clerk: In conjunction with the Troop or Detail PC Coordinator:
 - (1) Ensure that the laptop computer serial number and Division property number is placed on the assigned Members Accountability Record (form QM-2) when issued and removed when turned in.
 - (2) Inspect all laptop computers when they are turned in.
 - (3) Reissue serviceable laptops, and procur additional laptops as necessary.
 - (4) Return non-serviceable laptops to the Information Services Section at Division Headquarters for repair or replacement.
- (c) Laptops installed in UF patrol cars are to be used by all Members that use the vehicle. If the vehicle is removed from service, the laptop will be removed and installed in the replacement vehicle.
- (d) Division-issued software installed on the desktop and laptop will remain with the computer for the life of the computer or until updated, deleted, or replaced by the PC Coordinator or Information Services.
- (e) Accessories for the desktop and laptop will remain with the computer for the life of the computer.
- (f) Any equipment received from outside sources shall remain the property of the Troop, Detail, or Section where originally assigned.
- (g) Any laptop damaged in a FILE 3 Troop Car accident must be forwarded to the PC Coordinator for repair or replacement. The NYSPIN FILE 3 Message must note the condition of the laptop involved in the accident.

▣ (h) Disposal Of Equipment

Disposal of broken or outdated equipment is prohibited without proper authorization. Report the status of unserviceable technology equipment to the PC Coordinator.

PC Coordinator:

- ▣ (1) Prepare the appropriate documents for disposal of Division technology equipment and report the change in status of the equipment.
(SEE: Subsection titled: Inventory And Audit.)
- ▣ (2) Request replacement equipment.
- ▣ (3) Separate technology equipment into two categories: Non-hazardous equipment and Hazardous equipment.
 - ▣ • Non-hazardous equipment includes: Desktop computers, mice, keyboards, printers, etc. Non-hazardous equipment will be disposed of at the Troop level. The Troop PC Coordinator and Senior Stores Clerk will make arrangements with a local vendor for disposal.
 - ▣ † Remove the equipment from the Technology Information Management (TIM) system.
 - ▣ † Remove the hard drives from all computers identified for disposal and send the hard drives to the PC Support Unit at Division Headquarters along with the property number of the computer it was removed from. Hard drives will be wiped clean and destroyed by the PC Support Unit.
 - ▣ † Remove and retain all useable parts.
 - ▣ † Prepare and submit the Technology Equipment Transfer, Addition Or Disposal Record (form QM-26T) to the Division Quartermaster.
 - ▣ • Hazardous equipment includes: All batteries, CRT monitors and laptop computers. These items will be sent to Division Headquarters, PC Support Unit of Information Services for disposal.
 - ▣ † Contact the Help Desk to schedule delivery of hazardous equipment. A minimum of four weeks prior notice must be given.
 - ▣ † Prepare a Technology Equipment Transfer, Addition Or Disposal Record (form QM-26T) to accompany the items to be disposed of.
 - ▣ † Deliver the equipment to Division Headquarters and place in the area designated by Information Services. Give a copy of the Technology Equipment Transfer, Addition Or Disposal Record (form QM-26T) to a representative of the PC Support Unit.
 - ▣ † Remove the equipment from the Technology Equipment Inventory listing.

[IO 04-08 7/04]

NYSP Administrative Manual - Article 11

11Q5 Personal Computer Software(a) Licensing:

- (1) All software installed on Division equipment MUST be properly licensed.
- (2) Any unauthorized copying of licensed software is a violation of copyright laws and is strictly prohibited.

(b) Standard Software:

The Division has adopted standards in various software categories. Any of the standard software may be installed on Division computers by requesting the installation from the PC Coordinator. A list of standard software can be obtained by contacting the PC Coordinator or Information Services.

(c) Installation Of Non-Standard Software

- ☐ (1) Only approved software may be installed on Division computers. The purchase of, acquisition and/or implementation of non-standard software from outside sources to be used with any of Division's computer systems, networks or communications systems, requires approval from the Information Security Unit.
 - ☐ • Prepare and submit a request to install and/or implement non-standard software on Division technology equipment to the Information Security Unit at Division Headquarters and forward a copy of the request to your PC Coordinator.
 - ☐ • The request must justify the need and intended use of the non-standard software.
 - ☐ • If approval is granted, the PC Coordinator or Information Services will arrange for installation of the software.
- ☐ (2) The approved software will be registered with the PC Coordinator and Information services.
- ☐ (3) The software is to be used for State Police business only.

11Q6 Virus Protection

Computer viruses are hidden computer programs that can damage hardware and software and can result in the loss of data. Viruses are commonly spread by using an infected diskette in a PC, downloading infected software, or installing infected software. To reduce this risk, all users must follow the guidelines set forth in this policy regarding the installation of software. In addition:

- (a) All Division-issued computers are equipped with virus protection software.
- (b) The virus protection software installed will detect the most common viruses, but does not provide 100% protection against every possible virus variety.

- (c) Do not disable or alter the virus protection software installed on any Division computer without the direct approval of Information Services.
- (d) Follow prescribed procedures to update virus protection software when advised by the Information Services Section.

11Q7 Software Applications

- (a) A "software application" is defined as a specific task or set of tasks to be performed by a computer software package.
- (b) Applications may be either "Division-wide" or "site specific" (usage only applies to a single or a limited number of sites).
- (c) Prior to developing any Division-wide or site specific applications, the application must meet Division standards and approval must be received from the Information Services Section. After receiving approval for development of the application, the developer must adhere to the standards for developing systems and testing systems. A copy of these procedures can be obtained from the PC Coordinator or Information Services.
- (d) Applications developed in the standard Division software packages by the users can be registered with the Information Services staff to make them available Division-wide.
- (e) A current list of available forms and applications is available from the Troop PC Coordinator or Information Services at Division Headquarters.

11Q8 Internet/Acceptable Use Policy

(a) Introduction

The Division maintains a direct connection to the Internet that provides for a highly secure network, thereby minimizing potential system security risks, such as viruses and criminal activity.

Individual Internet accounts outside the Division Internet connection will only be made available by the Division on a case-by-case basis to those Employees who have a documented need for access outside the Division network.

Any misuse, abuse or any other inappropriate use of the Internet may result in removal of access to the Internet and/or disciplinary action.

No Employee may install or utilize personally-owned Internet software on Division equipment (i.e., AOL, Compuserve or Prodigy, etc.).

(b) Principles Of Acceptable Use

Internet access via Division computer equipment is for official business-related purposes such as efficiently exchanging information, conducting research on Division-related assignments, conducting investigations, obtaining documents/files in support of official responsibilities and professional development. In accordance with New York State standards for Internet access and use, New York State Police Employees with a Division-provided Internet account will:

- (1) Respect the privacy of others; for example, users shall not intentionally seek information on, obtain copies of, or modify files or data, belonging to other users, unless you have obtained explicit permission to do so;

NYSP Administrative Manual - Article 11

[IO 99-48 11/99]

- (2) Respect the legal protection provided to programs and data by copyright license;
- (3) Protect data from unauthorized use or disclosure as required by State and Federal laws and Division regulations;
- (4) Respect the integrity of computing systems; for example, users shall not use or develop programs that harass other users or infiltrate a computer or computing system and/or damage or alter the software components of the computer or computing system; and
- (5) Safeguard accounts and passwords. Any user changes of a password must follow guidelines for valid passwords. Accounts and passwords are normally assigned to single users and are not to be shared with any other person without authorization. Users are to report any actual or attempted security violations; and
- (6) When downloading files from the Internet, delays can be caused in network response time, as well as being infected with viruses. Any download that will require more than ten minutes must be approved by the PC Coordinator or Information Services. All downloaded files must be checked for viruses.

(c) Prohibited Usage:

Access to the Internet by any Employee of the Division must be consistent with this Internet Policy and its related E-mail Policy. Division Employees are prohibited from using Internet facilities for:

- (1) Activities unrelated to the mission of the New York State Police;
- (2) Activities violating Division Rules, Regulations or Instructions;
- (3) Unauthorized distribution of data and information;
- (4) Interfering with or disrupting network users, services or equipment; and
- (5) Activities related to personal gain.

(d) Division Rights:

The Division is not responsible for the loss of data resulting in delays, non-deliveries, or service interruptions caused by negligence, errors or omissions. Use of any information obtained via the Internet is at the user's risk. Any computer (standalone or connected to a Division network) must have anti-virus software installed. The Division makes no warranties, either expressed or implied, with regard to software obtained via the Internet.

The Division reserves the right to change its policies and rules with regard to Internet access at any time. The Division makes no warranties (expressed or implied) with respect to Internet service and specifically assumes no responsibilities for:

- (1) Content of any advice or information received by users or any costs or charges incurred as a result of seeking or accepting such advice.
- (2) Any costs, liabilities or damages caused by the way the user chooses to use his/her agency provided Internet account.

(e) Summary:

Questions about specific uses related to security issues not enumerated in this policy, and reports of specific unacceptable uses, should be directed to the PC Coordinator. Other questions about appropriate use should be directed through Channels to the Assistant Deputy Superintendent -- Technology and Planning.

The Division will review alleged violations of the Information Technology policies including the Internet Acceptable Use Policy and E-mail Policy on a case-by-case basis. Confirmed violations of the policy which are not promptly remedied will result in termination of Division-provided Internet services for the person(s) at fault, and referral for disciplinary action as appropriate.

11Q9

E-mail Policy(a) Introduction

Electronic mail, or E-mail, is becoming more widely available as an alternative to written and/or verbal communications. The New York State Police has long had electronic message sending/receiving capabilities via NYSPIN and MIN. The Division's Wide Area Network (WAN) links Division Headquarters, Troops, Zones and Stations with each other and with appropriate federal, state and local organizations, and provides authorized Division Employees with the standard Division e-mail software package.

E-mail accounts are provided by the Division to Employees who have a work-related need for electronic communication with other individuals either inside and/or outside the agency.

E-mail should be considered the same as written correspondence and is subject to the same standards, reviews, approvals, records retention and other normal practices.

No Division Employee may install or utilize E-mail or GroupWise software on Division equipment unless authorized by Information Services.

(b) Use Of E-mail

E-mail services, like other means of communication, are to be used to support Division business. Employees may use New York State Police computer equipment to communicate via E-mail with others in the Division as long as the communication meets professional standards of conduct. Personnel may use New York State Police computer equipment to communicate via E-mail outside of the Division when such communications are related to legitimate business activities and are within their professionally-related job assignments or responsibilities. Employees will not use E-mail for illegal, prohibited, unethical or unprofessional activities, or for personal gain, or political campaigns or for any purpose that would jeopardize the legitimate interests of the State, or constitute a violation of Division Rules, Regulations or Instructions.

Division Employees are prohibited from sending any type of mass mailing via E-mail statewide without first receiving permission from their Troop or Detail Commander or Division Headquarters Section Head. Employees should forward through Channels any information which is intended to be disseminated on a regional or statewide basis.

With the growth in use of electronic means to communicate, all Division Employees are responsible for reading E-mail messages on a regular basis - at least daily on all work days.

(c) Privacy And Use Considerations

Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC 2510, et seq.), notice is hereby given that there is no provision for sending or receiving private or confidential electronic communications. Messages relating to or in support of illegal or inappropriate activities will be reported to your immediate supervisor.

E-mail documents prepared by Division personnel may be read by persons other than those intended by the sender; this can happen unintentionally. While the Division does not routinely screen or read E-mail, supervisors may occasionally need to read a subordinate's E-mail, such as when they are away from the office, or it may be that a message is forwarded to a user for whom it was not originally intended, as well as for other reasons.

E-mail senders/receivers should likewise be aware of the fact the E-mail messages may be stored on remote hard disk drives and backup tapes; therefore, the deletion of an E-mail message by the sender or receiver may not result in its expungement. Also, E-mail sent to another computer system outside the Division may have a long life of its own on that system.

E-mail messages sent or received in conjunction with Division business may:

- (1) Be released to the public under the Freedom of Information Law; and
- (2) Require special measures to comply with the Personal Privacy Protection Law.
- (3) May be subject to discovery proceedings in legal actions, including personal communications.

Basically, senders/receivers of E-mail have a reduced expectation of privacy when compared to documents sent via US mail or comparable service providers. Similarly, E-mail senders/receivers have a reduced expectation of privacy compared to verbal communications conducted by telephone. This reduced expectation of privacy has been upheld in various court decisions.

(d) Acceptable Use Policy

The use of NYSP computer equipment to send/receive E-mail is intended for business-related purposes. E-mail sent/received via NYSP computer equipment is the property of the NYSP and as such the Division has the right to monitor and review the E-mail sent/received by its Employees. Although the NYSP does not intend to monitor and review E-mail on a routine basis, it will do so from time to time. All E-mail users should:

- (1) Follow accepted standards of etiquette in their messages;
- (2) Protect others' privacy and maintain confidentiality;
- (3) Not send messages which are harassing, sexually explicit, contain inappropriate language or can be interpreted as offensive to the receiver;
- (4) Send virus warnings and chain letters to the Division Help Desk only;
- (5) Not open attached files to E-mail messages if the receiver does not know the sender of the message. These types of messages should be forwarded to the Director of Information Services;
- (6) Not send sensitive information via Internet E-mail without first encrypting the message;
- (7) Limit the use of mass mailings to business-related topics only and the mass mailing must be approved by the Troop or Detail Commander;

- (8) Consider Division access before sending, filing, or destroying E-mail messages;
- (9) Protect their passwords;
- (10) Remove messages in a timely manner; and
- (11) Comply with New York State Police policies, procedures and standards.

§11Q10 Security

(a) Mission

The Information Technology Security mission is to safeguard the confidentiality, integrity and availability of information in all New York State Police systems. Information security will be the shared responsibility of the Division's Information Security Officer, the Information Security Unit, the Information Services Section, PC Coordinators, other designated staff and each system user.

By use of Division equipment and systems, users accept responsibility for knowing and complying with all pertinent laws, rules, regulations, policies and instructions including, but not limited to, security policies of the federal government, the Office for Technology and the Division of State Police. Users shall comply with all requirements including using, securing and changing passwords, other access and authorization codes or techniques, safeguarding and not divulging information to unauthorized persons, using virus protection software and reporting all security issues, breaches or violations.

The Division will review alleged violations of the Information Technology policies, including the Internet Acceptable Use Policy and E-mail Policy, on a case-by-case basis. Confirmed violations of the policy which are not promptly remedied will result in termination of Division-provided Internet services for the person(s) at fault. The person or persons involved are subject to disciplinary action as appropriate.

(b) Information Security Unit

The Information Security Unit (ISU) is under the direction of the Assistant Deputy Superintendent -- Technology and Planning, who is designated the New York State Police Information Security Officer (ISO).

The Information Security Unit (ISU) will be responsible for establishing policies and procedures and to ensure that the Division's security needs are met. The ISU will work in close coordination with the Information Services Section and other Division Sections, as appropriate.

The functional tasks and areas of responsibility of the ISU include, but are not limited to:

- Establishing and maintaining access control policies.
- Establishing and maintaining an information security testing and evaluation program.
- Ensuring overall compliance with the Division's information security requirements.
- Implementing and administering an information security risk assessment program.
- Ensuring that hardware and software in use by Employees meets our security requirements.

11R OTHER ADMINISTRATIVE REFERENCES

11R1 T-SLED Traffic Ticket Records [CROSS REFERENCE: Article 17 -- TICKETS.]

EXHIBIT D

NEW YORK STATE POLICE

MEMORANDUM

Troop H Station MHDETf

Date 03-19-07

To: Major John J. McCabe, CNET Headquarters, Albany, NY

From: Investigator Phil Etkin 

Subject: Security of Division Vehicle (Off Duty)

Writer is assigned the following vehicle: 2001 Ford Taurus color Brown, bearing NY registration ~~REDACTED~~. Said vehicle will be parked and secured off duty hours at the following address: ~~REDACTED~~ Rock Hill, NY ~~REDACTED~~. Said vehicle will be parked at writers temporary place of residence, in the driveway, visible from said residence. This memo supercedes old memo dated 01-17-07.